Tle

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/735,412	12/12/2003	Marc B. Dombrowa	YOR920030348US1	2134

34663 7590 11/16/2007

MICHAEL J. BUCHENHORNER
8540 S.W. 83 STREET
MIAMI, FL 33143

EXAMINER	
TRUONG, LOAN	
ART UNIT	**PAPER NUMBER**
2114	

NOTIFICATION DATE	DELIVERY MODE
11/16/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

MICHAEL@BUCHENHORNER.COM
ANA@BUCHENHORNER.COM

Office Action Summary	Application No.	Applicant(s)
	10/735,412	DOMBROWA ET AL.
	Examiner	Art Unit
	LOAN TRUONG	2114

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 June 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-6,9-16 and 18-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6,9-16 and 18-28* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in response to the amendment filed June 22, 2007 in application 10/735,412.

2. Examiner acknowledged that claims 1-6, 9-16, 18-28 are presented for examination; Claims 1, 6, 9-10, 11, 18 and 23 have been amended. Claims 7-8, 17 and 29 have been cancelled.

Response to Arguments

3. Applicant's arguments with respect to claims 1-6, 9-16, 18-28 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* v. *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

4. Claims 1-4, 9, 18-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Brothers et al. (US 6,789,182) in further view of Lenny et al. (US 6,600,614) in further view of Koike (US 6,801,138).

In regard to claim 1, Brothers et al. teach a distributed network comprising:

A plurality of processor (*Target processors, fig. 2, 210 a-c*);

A local counter (*time stamp clock, fig. 1, 120, applicant's specification refer to that counter as a holding a synchronized global clock/counter synchronizer, page 6 lines 8-10)* associated with each of the processors (*Target processors, fig. 2, 210 a-c)* in the distributed network (*distributed system, col. 3 lines 33-40)*;

An event register (*event memory, fig. 1, 110)* associated with each of the local counters (*time stamp clock, fig. 1, 120)*;

An event logger (*collection control unit, fig. 1, 115)* for receiving a counter value (*time tag, fig. 6, 610),* from the local counter (*time stamp clock, fig. 1, 120)* in response to an event (*event received from target, fig. 6, 610)* being registered in the event register (*event memory, fig. 1, 110)*; and

Brothers et al. does not explicitly teach a distributed network comprising of software for performing conditional probability calculations based on event information stored in a history table wherein the conditional probability calculations are performed to determine if a probability of an event occurring has exceeded a minimum threshold level

and, if the threshold is exceeded, to migrate a process or schedule maintenance to avoid consequences of a predicted event;

Lenny et al. teach the critical event log wherein SMART is a reliability predictive technology for predicting or anticipating a failure *(col. 5 lines 61-67)* wherein SMART only record events or errors types that exceeds the established minimum threshold that is useful for predicting failure *(col. 7 lines 49-56)*.

It would have been obvious to modify the system of Brothers et al. by adding Lenny et al. teach the method of critical event log. A person of ordinary skill in the art at the time of applicant's invention would have been motivated to make the modification because it would provide a technique to log critical events that are useful for conducting a failure analysis and show the operational history prior to the failure *(col. 2 lines 49-55)*.

Brothers et al. and Lenny et al. does not explicitly teach a distributed network comprising of software wherein the conditional probability calculations are based upon events occurring within a selected time window.

Koike teach the positional data utilizing inter-vehicle communication by implementing a calculation of collision probability between receiving vehicle and user's vehicle in space-time and magnitude of impact shock of crash *(fig. 26, s206, fig. 27, s207)*.

It would have been obvious to modify the system of Brothers et al. and Lenny et al. by adding Koike positional data communication. A person of ordinary skill in the art at the time of applicant's invention would have been motivated to make the modification

because it would allow precise information to be obtained to assist carrying out of accurate avoidance control (*col. 2 lines 40-44).*

In regard to claim 2, Brothers et al. disclosed the distributed network of claim 1 comprising a global clock (*the time stamp clock of one of the event collection cards acts as a master synchronization clock that synchronizes clocks of the other event collection cards, col. 7 lines 60-63)* wherein a time stamp is calculated based on the counter value received from a counter (*time stamp clock, fig. 1, 120)* associated with a processor (*Target processors, fig. 2, 210 a-c)* in the distributed network (*distributed system, col. 3 lines 33-40).*

In regard to claim 3, Brothers et al. disclosed the distributed network of claim 1 wherein the event logger (*collection control unit, fig. 1, 115)* records data concerning a type of event registered by the event register and a time an event occurred (*received event from target and time tag and store event, fig. 6, 610, 620).*

In regard to claim 4, Brothers et al. disclosed the distributed network of claim 1 wherein the event register (*event memory, fig. 1, 110)* remains frozen until the event register is read by the system monitor (*event count interrupt signifying that event memory has reached a predetermined storage threshold, col. 12 lines 11-19).*

In regard to claim 9, Brothers et al. disclosed the distributed network of claim 1 wherein the event register (*event memory, fig. 1, 110)* comprises an error time stamp register (*stored time-*

stamped event information in event storage memory, col. 6 lines 15-20) that receives a value from the local counter (*time stamp clock, fig. 1, 120)* when an event occurs (*time tag, fig. 6, 620).*

In regard to claim 18, Brothers et al. disclosed a distributed computer system for implementing a time stamping process for producing a time stamp associated with an occurrence of an error event, the computer system comprising:

A plurality of processors (*Target processors, fig. 2, 210 a-c)*;

A plurality of local counters (*time stamp clock, fig. 1, 120)* wherein each counter is associated (*fig. 1 shows only one event collection card, present invention includes multiple cards synchronized together to collect event from distributed processors, col. 4 lines 54-58)* with one of the plurality of processors (*Target processors, fig. 2, 210 a-c*) in the distributed computer system (*distributed system, col. 3 lines 33-40)*;

An event register (*event memory, fig. 1, 110)* for recording event information concerning an occurrence of an event associated with the processor (*received event from target, fig. 6, 610)* and event register (*store information in event memory, col. 11 lines 56-59)*;

An event logger (*collection control unit, fig. 1, 115)* for receiving a counter value (*time tag, fig. 6, 610),* from the local counter (*time stamp clock, fig. 1, 120)* in response to an event (*event received from target, fig. 6, 610)* being registered in the event register (*event memory, fig. 1, 110)*; and

Brothers et al. does not explicitly teach a distributed network comprising of software for performing conditional probability calculations based on event information stored in a history table wherein the conditional probability calculations are performed to

determine if a probability of an event occurring has exceeded a minimum threshold level and, if the threshold is exceeded, to migrate a process or schedule maintenance to avoid consequences of a predicted event;

Lenny et al. teach the critical event log wherein SMART is a reliability predictive technology for predicting or anticipating a failure (*col. 5 lines 61-67*) wherein SMART only record events or errors types that exceeds the established minimum threshold that is useful for predicting failure (*col. 7 lines 49-56*).

Refer to claim 1 for motivational statement.

Brothers et al. and Lenny et al. does not explicitly teach a distributed network comprising of software wherein the conditional probability calculations are based upon events occurring within a selected time window.

Koike teach the positional data utilizing inter-vehicle communication by implementing a calculation of collision probability between receiving vehicle and user's vehicle in space-time and magnitude of impact shock of crash (*fig. 26, s206, fig. 27, s207*).

Refer to claim 1 for motivational statement.

In regard to claim 19, Brothers et al. disclosed the distributed computer system of claim 18 comprising a global clock for synchronizing the local counters (*the time stamp clock of one of the event collection cards acts as a master synchronization clock that synchronizes clocks of the other event collection cards, col. 7 lines 60-63*).

In regard to claim 20, Brothers et al. disclosed the distributed computer system of claim 19 wherein the event logger (*collection control unit, fig. 1, 115)* records a time stamp based upon the global clock (*the time stamp clock of one of the event collection cards acts as a master, col. 7 lines 60-63)* and a local counter value received from a local counter (*time tag, fig. 6, 620).*

****

5. Claims 5-6, 10 and 21-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Brothers et al. (US 6,789,182) in further view of Lenny et al. (US 6,600,614) in further view of Koike (US 6,801,138) in further view of Lewis (US 6,430,712).

In regard to claim 5, Brothers et al., Lenny et al. and Koike does not teach the distributed network of claim 1 comprising dynamic masking mechanisms for filtering the event register outputs to differentiate between critical and non-critical events.

Lewis teaches the apparatus for inter-domain alarm correlation by implementing an alarm filtering for certain events to generate an alarm (*col. 2 lines 42-45).*

It would have been obvious to modify the system of Brothers et al., Lenny et al. and Kibkalo et al. by adding Lewis apparatus for inter-domain alarm correlation. A person of ordinary skill in the art at the time of applicant's invention would have been motivated to make the modification because it would resolve the overall issues with an increasing complex and larger network that traditionally would required a highly-skilled network administrator to provide a systematize the knowledge of networking expert so

that common problems can be detected, isolated and repaired automatically or by a less-skilled personnel *(col. 2 lines 15-45).*

In regard to claim 6, Brothers et al., Lenny et al. and Koike does not teach the distributed network of claim 5 wherein the masking is dynamically updated during online processing.

Lewis teaches the apparatus for inter-domain alarm correlation by implementing an alarm filtering for certain events to generate an alarm *(col. 2 lines 42-45)* in a communication network *(col. 3 lines 30-42).*

Refer to claim 5 for motivational statement.

In regard to claim 10, Brothers et al., Lenny et al. and Koike does not teach the distributed network of claim 1 wherein the event register stores an error occurred value that indicates to the network monitor that a critical event has occurred.

Lewis teaches the apparatus for inter-domain alarm correlation by implementing an alarm filtering for certain events to generate an alarm *(col. 2 lines 42-45)* by correlating to determined a severity of a condition *(col. 3 lines 61-67).*

Refer to claim 5 for motivational statement.

In regard to claim 21, Brothers et al., Lenny et al. and Koike does not teach the distributed computer system of claim 18 comprising dynamic masks created based upon historical event information for filtering events such that only information concerning critical events result is stored.

Lewis teaches the apparatus for inter-domain alarm correlation by implementing an alarm filtering for certain events to generate an alarm *(col. 2 lines 42-45)*.

Refer to claim 5 for motivational statement.

In regard to claim 22, Brothers et al. does not teach the distributed computer system of claim 21 comprising software for evaluating events based on conditional probabilistic calculations and scheduling remedial or preventative action during online processing.

Lenny et al. teach the method of critical event log wherein SMART is a reliability predictive technology for predicting or anticipating a failure *(col. 5 lines 61-67)* wherein SMART monitors a series of attributes that are indicators of an electronic or mechanical component failure *(col. 6 lines 6-10)*. Furthermore, SMART generates alarm signal and if the report status signal imminent failure, the host computer sends an alarm to the end user or the system administrator for schedule of downtime, backup data and replacement of the disk drive *(col. 6 lines 18-27)*.

Refer to claim 1 for motivational statement.

****

6. Claims 11, 23 and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Brothers et al. (US 6,789,182) in further view of Koike (US 6,801,138).

In regard to claim 11, Brothers et al. teach a method of producing a time stamp for an event occurring on a distributed network, the method comprising:

Producing a local counter value (*time tag, fig. 6, 620)* for each of a plurality of processors (*Target processors, fig. 2, 210 a-c)* in the distributed network (*distributed system, col. 3 lines 33-40)* with an associated counter (*time stamp clock, fig. 1, 120)*;

Synchronizing the local counter at each of the processors with a global clock (the time stamp clock of one of the event collection cards acts as a master synchronization clock that synchronizes clocks of the other event collection cards, col. 7 lines 60-63); and

Freezing the local counter for a processor when a critical event associated with the processor occurs (*event count interrupt signifying that event memory has reached a predetermined storage threshold, col. 12 lines 11-19*),

Brothers et al. does not teach a method comprising dynamically masking events that occur based on conditional probabilistic calculations using machine learning algorithms to predict an occurrence of a critical event during a specified time period.

Koike teach the positional data utilizing inter-vehicle communication by implementing a calculation of collision probability between receiving vehicle and user's vehicle in space-time and magnitude of impact shock of crash (*fig. 26, s206, fig. 27, s207)* wherein the present position and projected positions at two seconds later, four seconds later, ..., n seconds later are represented in the form of time data and positional data, and communication pattern is determined based on these data (*col. 2 lines 10-22)*.

It would have been obvious to modify the system of Brothers et al. by adding Koike positional data communication. A person of ordinary skill in the art at the time of

applicant's invention would have been motivated to make the modification because it would allow precise information to be obtained to assist carrying out of accurate avoidance control *(col. 2 lines 40-44).*

In regard to claim 23, Brothers et al. disclosed a computer-executable medium comprising instructions for producing a time stamp for an event occurring on a distributed network including a plurality of processors, the medium comprising instructions for:

Producing a local counter value *(time tag, fig. 6, 620)* for each of a plurality of processors *(Target processors, fig. 2, 210 a-c)* in the distributed network *(distributed system, col. 3 lines 33-40)* with an associated counter *(time stamp clock, fig. 1, 120)*;

Synchronizing the local counter at each of the processors with a global clock (the time stamp clock of one of the event collection cards acts as a master synchronization clock that synchronizes clocks of the other event collection cards, col. 7 lines 60-63);

Freezing the local counter for a processor when a critical event associated with the processor occurs (event count interrupt signifying that event memory has reached a predetermined storage threshold, col. 12 lines 11-19); and

Brothers et al. does not teach a method comprising dynamically masking events that occur based on conditional probabilistic calculations using machine learning algorithms.

Koike teach the positional data utilizing inter-vehicle communication by implementing a calculation of collision probability between receiving vehicle and user's vehicle in space-time and magnitude of impact shock of crash *(fig. 26, s206, fig. 27,*

s207) wherein the present position and projected positions at two seconds later, four seconds later, ..., n seconds later are represented in the form of time data and positional data, and communication pattern is determined based on these data *(col. 2 lines 10-22).*

Refer to claim 11 for motivational statement.

In regard to claim 25, Brothers et al. disclosed the medium of claim 23 comprising an instruction for periodically polling the local counters and storing information received in a history table (*CPU may read the event count on a periodic basis when sending the formatted events to host computer, fig. 7, 730, col. 12 lines 11-15).*

****

7. Claims 12-16, 24 and 27-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Brothers et al. (US 6,789,182) in further view of Koike (US 6,801,138) in further view of Lenny et al. (US 6,600,614).

In regard to claim 12, Brothers et al. and Koike does not teach the method of claim 11 comprising establishing a history table containing information concerning events associated with the critical event and the conditional probabilities of the associated events during offline processing.

Lenny et al. teach the method of critical event log wherein the off-line data collection mode is performed to log events corresponding to predefined critical events *(TABLE 3, col. 11 lines 26-32).* Furthermore, SMART is a reliability predictive

technology for predicting or anticipating a failure (*col. 5 lines 61-67)* wherein SMART Error Logging is an extension of SMART for reporting a record of the most recent errors (*col. 6 lines 36-42).*

It would have been obvious to modify the system of Brothers et al. and Koike by adding Lenny et al. teach the method of critical event log. A person of ordinary skill in the art at the time of applicant's invention would have been motivated to make the modification because it would provide a technique to log critical events that are useful for conducting a failure analysis and show the operational history prior to the failure (*col. 2 lines 49-55).*

In regard to claim 13, Brothers et al. and Koike does not teach the method of claim 12 comprising determining during an offline phase if an event is critical and whether or not online processing is possible.

Lenny et al. teach the method of critical event log wherein the off-line data collection mode is performed to log events corresponding to predefined critical events (*TABLE 3, col. 11 lines 26-32).* Furthermore, SMART is a reliability predictive technology for predicting or anticipating a failure (*col. 5 lines 61-67)* wherein SMART Error Logging is an extension of SMART for reporting a record of the most recent errors (*col. 6 lines 36-42).*

Refer to claim 12 for motivational statement.

In regard to claim 14, Brothers et al. and Koike does not teach the method of claim 12 comprising dynamically filtering the events based on a recorded history of information associated with the occurrence of events such that only certain critical events produce global interrupts.

Lenny et al. teach the method of critical event log wherein SMART is a reliability predictive technology for predicting or anticipating a failure *(col. 5 lines 61-67)* wherein SMART monitors a series of attributes that are indicators of an electronic or mechanical component failure. These attributes are chosen specifically for each individual model *(col. 6 lines 6-10).*

Refer to claim 12 for motivational statement.

In regard to claim 15, Brothers et al. and Koike does not teach the method of claim 12 comprising updating the conditional probability information and history table during offline processing.

Lenny et al. teach the method of critical event log wherein the off-line data collection mode is performed to log events corresponding to predefined critical events *(TABLE 3, col. 11 lines 26-32)* in SMART Error Logging *(col. 6 lines 39-42).*

Refer to claim 12 for motivational statement.

In regard to claim 16, Brothers et al. teach the method of claim 11 comprising determining a type of event that occurred and determining whether to produce a synch stop *(if*

clock reaches the preset time before the sync signal is received, then sync control unit may stop time stamp clock until the sync signal is received, col. 10 lines 58-64).

Brothers et al. and Koike does not teach the method of claim 11 comprising determining during online processing a type of events that occurred and determining whether to produce a global alert or machine check alert signal based upon the type of event that occurred.

Lenny et al. teach the method of critical event log wherein the off-line data collection mode is performed to log events corresponding to predefined critical events (*TABLE 3, col. 11 lines 26-32)* in SMART Error Logging (*col. 6 lines 39-42).* Furthermore, SMART generates alarm signal and the software on the host computer interprets the alarm signals, the host then sends an alarm to the end user or the system administrator to allow for scheduling downtime for backup of data and replacement (*col. 6 lines 18-27).*

Refer to claim 12 for motivational statement.

In regard to claim 24, Brothers et al. teach the medium of claim 23 comprising an instruction for monitoring the local counter (*local time counter, fig. 1)* with a system monitor (*event collection card, fig. 2, 200 a-c)* through the use of online and offline processing.

Brothers et al. and Koike does not teach the medium for monitoring through the use of online and offline processing.

Lenny et al. teach the method of critical event log wherein SMART is a reliability predictive technology for predicting or anticipating a failure (*col. 5 lines 61-67)* wherein SMART Critical Event Logging operations during on-line and off-line mode (*col. 10 lines 32-48).*

Refer to claim 12 for motivational statement.

In regard to claim 27, Brothers et al. and Koike does not teach the medium of claim 23 comprising an instruction for performing conditional probability calculations to determine if a probability that a critical event will occur exceeds a threshold level and performing or scheduling preventative action if such threshold is exceeded.

Lenny et al. teach the method of critical event log wherein SMART is a reliability predictive technology for predicting or anticipating a failure (*col. 5 lines 61-67)* wherein SMART only record events or errors types that exceeds the established minimum threshold that is useful for predicting failure (*col. 7 lines 49-56).*

Refer to claim 12 for motivational statement.

In regard to claim 28, Brothers et al. teach the medium of claim 11 comprising an instruction for determining a type of event that occurred (*event a-e, fig. 2, 240)* and determining whether to produce a synch stop (*if clock reaches the preset time before the sync signal is received, then sync control unit may stop time stamp clock until the sync signal is received, col. 10 lines 58-64).*

Brothers et al. and Koike does not teach the method of claim 11 comprising determining whether to produce a global alert or machine check alert signal based upon the type of event that occurred.

Lenny et al. teach the method of critical event log wherein the off-line data collection mode is performed to log events corresponding to predefined critical events (*TABLE 3, col. 11 lines 26-32*) in SMART Error Logging (*col. 6 lines 39-42*). Furthermore, SMART generates alarm signal and the software on the host computer interprets the alarm signals, the host then sends an alarm to the end user or the system administrator to allow for scheduling downtime for backup of data and replacement (*col. 6 lines 18-27*).

Refer to claim 12 for motivational statement.

****

8. Claim 26 is rejected under 35 U.S.C. 103(a) as being unpatentable over Brothers et al. (US 6,789,182) in further view of Koike (US 6,801,138) in further view of Lewis (US 6,430,712).

In regard to claim 26, Brothers et al. and Koike does not teach the medium of claim 23 comprising an instruction for dynamically filtering the events based on a recorded history of information associated with the occurrence of events such that only critical events are reported to a system monitor.

Lewis teaches the apparatus for inter-domain alarm correlation by implementing an alarm filtering for certain events to generate an alarm *(col. 2 lines 42-45).*

It would have been obvious to modify the system of Brothers et al. by adding Lewis apparatus for inter-domain alarm correlation. A person of ordinary skill in the art at the time of applicant's invention would have been motivated to make the modification because it would resolve the overall issues with an increasing complex and larger network that traditionally would required a highly-skilled network administrator to provide a systematize the knowledge of networking expert so that common problems can be detected, isolated and repaired automatically or by a less-skilled personnel *(col. 2 lines 15-45).*

****

Conclusion

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO 892.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Loan Truong whose telephone number is (571) 272-2572. The examiner can normally be reached on M-F from 8am-4pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Scott Baderman can be reached on (571) 272-3644. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Loan Truong
Patent Examiner
AU 2114

SCOTT BADERMAN
SUPERVISORY PATENT EXAMINER